AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

United States of America
v.
RYAN MARK GINSTER

Case No.3:21-mj-71802 MAG

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of February 2018 to Febraury 2021 in the county of San Francisco in the Northern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1343	Count 1: Wire Fraud
18 U.S.C. § 1956(a)(1)(B)(i)	Counts 2-7: Engaging in Monetary Transactions to Conceal or Disguise

This criminal complaint is based on these facts:

See affidavit by Special Agent Jeremiah Haynie attached.

☑ Continued on the attached sheet.

/s/
Complainant's signature

Special Agent Jeremiah Haynie, IRS-CI
Printed name and title

Approved as to form David J. Ward
AUSA David J. Ward

Sworn to before me by telephone.

Date: November 16, 2021

Judge's signature

City and state: San Francisco, CA

Hon. Jacqueline Scott Corley
Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Jeremiah Haynie, being duly sworn, state:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a criminal complaint against RYAN MARK GINSTER ("GINSTER").

2. In summary, this affidavit describes a scheme to defraud orchestrated by GINSTER through various websites that offered investors very high rates of return, as high as 5% per day, by purportedly using the funds for various financial or online marketing efforts. Each of the various "investment" sites were short-lived and shut down without repaying investors, including the investments raised through "Socialprofimatic.com," which shut down after 38 days. GINSTER took efforts to hide his involvement in all the investment sites, and I rely on non-public documents and evidence described below to link GINSTER to the anonymous sites, including IP address information, domain name purchase records, bank records, cryptocurrency exchange account information, and cryptocurrency transaction information discovered in search of his residence. GINSTER also knowingly transferred the proceeds of the scheme through various accounts, including through a cryptocurrency exchange into his personal bank account.

3. I am a Special Agent with the Criminal Investigation Division of the Internal Revenue Service ("IRS-CI") and have been so employed since February 2002. My professional duties include conducting investigations of violations of internal revenue laws and related statutes. I hold a bachelor's degree in business administration from Alma College. I have been trained at the Federal Law Enforcement Training Center in criminal tax, fraud, and money laundering, as well as the use of search warrants and criminal complaints. As a federal agent, I

am authorized to investigate violations of laws of the United States and to execute arrest and search warrants issued under the authority of the United States. I have been the affiant for numerous federal criminal complaint, search warrant, and seizure warrant affidavits that involved varied criminal conduct including alleged tax violations, money laundering, unlicensed money transmitting business violations, wire fraud, access device fraud, and mail fraud.

4. As an IRS-CI Special Agent, I have received extensive financial records analysis training and attended mandated continuing professional education courses on investigative techniques and methods utilized in the investigation of violations of tax, fraud, and money laundering statutes. I have participated in and led many investigations involving alleged violations of tax, fraud, and money laundering laws. Since 2015, I have been assigned to the IRS-CI Cyber Crimes Unit where I have received training and gained experience investigating criminal schemes perpetrated via the internet, including schemes executed with the use of cryptocurrencies. I rely on my experience and evidence obtained in presenting the facts below.

5. I am familiar with the information contained in this affidavit based on my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers and civilian witnesses. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. I have set forth facts that I believe are necessary to establish probable cause.

GLOSSARY

Bitcoin

6. Bitcoin is a form of financial value that is transacted via the Internet. Bitcoin is described as a "decentralized" currency because no particular entity or individual has control of the Bitcoin network. Instead, thousands of individuals across the world run Bitcoin software. The software provides all services necessary for Bitcoin to function, including allowing users to securely transfer bitcoin,[1] the injection of new bitcoin into circulation; and the creation of new "bitcoin addresses," roughly equivalent to account numbers. For security and privacy reasons, it is common for a single bitcoin user to control numerous bitcoin addresses, which may be accessed and controlled through the user's "bitcoin wallet." When reference is made to the U.S. dollar value of bitcoin, I used CoinDesk.com to determine the approximate price of bitcoin on the day of the transfer, unless otherwise noted.

Bitcoin Attribution

7. Because bitcoin addresses contain no information that identifies the owner of the address, bitcoin transactions by themselves are generally considered anonymous. Discovery of the owner of a bitcoin address can occur when the owner provides the bitcoin address while requesting payment or uses the bitcoin address to make a payment. Analysis of the spending history of a bitcoin address can reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many bitcoin addresses to receive payments from different customers. When the business transfers the bitcoin that it has received, it may

[1] Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular, with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (singular, with a lowercase letter b) to label units of the currency. That practice is adopted here.

group those addresses together to send a single transaction. Analysis of the blockchain information associated with such a transaction would indicate that each of those addresses was, in fact, part of a "cluster" of bitcoin addresses controlled by a single entity. This analysis allows law enforcement and the private sector alike to gain insight into all of the addresses associated with an entity. Several companies specializing in blockchain analysis create large databases for building these clusters and offer software products to facilitate this sort of analysis.

Virtual Currency Exchangers

8. Virtual currency exchangers are in the business of buying virtual currencies from their customers, selling virtual currencies to their customers, and trading virtual currencies for other virtual currencies offered by their customers. Virtual currencies are electronic representations of value that can be transacted among accountholders. Coinbase, Inc., based in San Francisco, California, is an example of a virtual currency exchanger.

IP Address

9. A device's Internet Protocol address (IP address) is a unique numeric address used to direct information over the Internet. IPv4 addresses are written as a series of four groups of numbers, each in the range 0 – 255, separated by periods (e.g. 192.168.0.1). Conceptually, IP addresses are similar to telephone numbers in that they are used to identify devices that send and receive information over the Internet. Used within this context, a device is anything that can communicate over the Internet, including desktop computers, laptop computers, smartphones, routers, website servers, and even Internet-capable home appliances.

High Yield Investment Programs (HYIPs)

10. HYIPs promise outlandishly high returns with little or no risk to the investor. The typical lifecycle of a HYIP begins with the creation of a website that presents a fictious story

about how the HYIP generates income. For example, the HYIP may claim to use investor funds to develop an Internet advertising network that earns the investor a large percentage return on their investment. But instead of using the funds to invest in the presented opportunity, the HYIP owner uses a portion of the funds to pay current investors in order to keep them from blowing the whistle while new investors deposit funds. At some point during the lifecycle, the investor deposits wane and the owner of the HYIP stops interest payments to the investors, does not allow the investor to withdraw their original investment, and pockets the remaining funds. In order to entice others to market the HYIP, many HYIP operators set up a referral system that pays recruiters to solicit others for the investment opportunity. The recruiter receives a percentage of the amount the recruited investor deposits.

COUNT ONE: WIRE FRAUD (18 U.S.C. § 1343)

11. Beginning on a date unknown, but no later than February 2018, and continuing until on or about February 23, 2021, in the Northern District of California and elsewhere, defendant GINSTER knowingly, and with the intent to defraud, participated in, devised, and intended to devise, a scheme and artifice to defraud, by means of materially false and fraudulent pretenses, representations, and promises, and by means of omission and concealment of material facts. On or about March 6, 2018, in the Northern District of California and elsewhere, for the purpose of executing the aforementioned scheme and artifice to defraud and attempting to do so, the defendant did knowingly transmit and cause to be transmitted in interstate commerce, by means of a wire communication, certain writings, signs, signals, pictures, and sounds; specifically, a transfer of bitcoin from a Coinbase account conducted by an individual in the Northern District of California (Victim R.K.), into a bitcoin wallet controlled by GINSTER, in violation of Title 18, United States Code, Section 1343.

COUNT ONE:

03/06/2018	**Wire Transfer of 0.0468793 Bitcoin from Victim R.K. to GINSTER's Bitcoin Wallet**	**$502.06**

COUNTS TWO - SEVEN: ENGAGING IN MONETARY TRANSACTIONS TO CONCEAL OR DISGUISE (18 U.S.C. § 1956(a)(1)(B)(i))

12. Beginning on a date unknown, but no later than March 2018, and continuing until on or about February 23, 2021, in the Northern District of California and elsewhere, defendant GINSTER did conduct financial transactions with the proceeds of wire fraud, a specified unlawful activity, with the intent to conceal or disguise the nature, location, source, ownership or control of the proceeds. Specifically, GINSTER made three transfers of bitcoin received as a result of the wire fraud scheme described herein, moving the cryptocurrency from a bitcoin wallet on his computer (called "mainwallet") to his account at Coinbase, a cryptocurrency exchanger in the Northern District of California. Substantially all funds in "mainwallet" appear to be investments in Socialprofimatic.com. Hours after each transfer into his Coinbase account, GINSTER then converted a portion of these proceeds of wire fraud into U.S. dollars and made three transfers of those funds into a bank account in GINSTER's name at Carrollton Bank. (hereinafter "personal bank account"). GINSTER executed these six transactions with the knowledge that the funds were derived from proceeds of wire fraud.

a. On or about March 3, 2018, GINSTER's Coinbase account received 1.91626469 bitcoin, then worth $17,035, directly from a bitcoin wallet on GINSTER's computer called "mainwallet." On or about the same day, GINSTER converted 1.12356079 bitcoin to $9,851 and transferred the funds into his personal bank account at Carrollton Bank.

COUNT TWO:

Date	From	To	Amount
03/21/2018 18:51 UTC	**Social Profimatic Wallet ("mainwallet")**	**Ginster Coinbase Account**	**1.91626469 BTC ($17,035.61)**

COUNT THREE:

Date	From	To	Amount
03/21/2018 21:31 UTC	**Ginster Coinbase Account**	**Carrollton Bank Account**	**$9,851.00**

b. On or about March 23, 2018, GINSTER's Coinbase account received 1.15486691 bitcoin, then worth $9,695, directly from a bitcoin wallet on GINSTER's computer called " mainwallet." On the same day, GINSTER converted 2.33557851 in bitcoin to $19,702 and transferred the funds into his personal bank account at Carrollton Bank.

COUNT FOUR:

Date	From	To	Amount
03/23/2018 6:13 UTC	**Social Profimatic Wallet ("mainwallet")**	**Ginster Coinbase Account**	**1.15486691 BTC ($9,695.10)**

COUNT FIVE:

Date	From	To	Amount
03/23/2018 15:42 UTC	**Ginster Coinbase Account**	**Carrollton Bank Account**	**$19,702.00**

c. On or about March 24, 2018, GINSTER's Coinbase account received 2.4179672 bitcoin, then worth $20,987, from a bitcoin wallet on GINSTER's computer called "mainwallet." On or about March 25, 2018, GINSTER converted 2 bitcoin to $16,882.51, and transferred the funds into his personal bank account at Carrollton Bank.

COUNT SIX:

Date	From	To	Amount
03/24/2018 22:02 UTC	**Social Profimatic Wallet ("mainwallet")**	**Ginster Coinbase Account**	**2.4179672 BTC ($20,987.17)**

COUNT SEVEN:

Date	From	To	Amount
03/25/2018 21:10 UTC	**Ginster Coinbase Account**	**Carrollton Bank Account**	**$16,882.51**

RELEVANT LAW

13. **Title 18, United States Code, Section 1343** prohibits wire fraud. The elements of this offense are: 1) the defendant knowingly participated in, devised, or intended to devise, a scheme or plan to defraud, or a scheme or plan for obtaining money or property by means of false or fraudulent pretenses, representations, or promises; 2) the statements made or facts omitted as part of the scheme were material, that is they had a natural tendency to influence, or were capable of influencing, a person to part with money or property; 3) the defendant acted with the intent to defraud, that is, the intent to deceive or cheat; and 4) the defendant used, or caused to be used, a wire communication to carry out, or attempt to carry out an essential part of the scheme. See Ninth Circuit Model Criminal Jury Instruction 8.124.

14. **Title 18, United States Code, Section 1956(a)(1)(B)(i)** prohibits the laundering of proceeds from "specified unlawful activity" (SUA). The essential elements are 1) the defendant conducted or intended to conduct a financial transaction involving property that represented the proceeds of specified unlawful activity; 2) the defendant knew that the property represented the proceeds of specified unlawful activity; 3) the defendant knew the transaction was designed in whole or in part to conceal or disguise the nature, location, source, ownership, or

control of the proceeds of the specified unlawful activity; and 4) the defendant did something that was a substantial step toward committing the crime. See Ninth Circuit Model Criminal Jury Instruction 8.147. The money laundering statute specifically identifies § 1343 wire fraud as a "specified unlawful activity".

THE DEFENDANT

15. GINSTER, is a resident of Corona, CA. This investigation has determined that since at least 2018, GINSTER has been operating HYIP websites that solicit investments with fictitious claims of unrealistic gains, then absconding with much of the investment proceeds.

THE SCHEME TO DEFRAUD

I. Overview

16. Beginning no later than February 2018, and continuing to no later than February 2021, GINSTER created and ran HYIP websites, including a website he created and maintained called Socialprofimatic.com (hereafter, "**Subject Website**"), to communicate false representations for the purpose of defrauding investors. The **Subject Website** communicated material misrepresentations about investment opportunities, attracting cryptocurrency "investments" valued at the time at approximately $844,667.93.

17. The **Subject Website** included false representations regarding the investment, including that it would pay exorbitant (but unsustainable) rates of return, that the invested funds would be used to fund social media marketing campaigns, and that investors would be able to withdraw invested funds at any time.

18. GINSTER directed investors to unconventional methods of payment for the purchase of shares. The **Subject Website** did not accept traditional methods of payment such as bank transfers or credit cards. While the **Subject Website** was active, the accepted methods of

payment were Bitcoin, Bitcoin Cash, Litecoin, Doge Coin, Dash, and Ethereum. These are all like Bitcoin because they are decentralized, meaning there is no central authority to perform Know Your Customer or anti-money laundering controls. From my training and experience, I know that fraudulent online investment schemes typically use one or more of these payment methods because transactions are irrevocable, meaning that once a transaction is executed, it cannot be reversed, even in instances of fraud. This is unlike a bank or credit card transaction which can be reversed when fraudulent transactions are discovered. In addition, by design, these cryptocurrencies do not require their users to provide any verified identifying information to execute transactions and are frequently used for fraud.

19. As detailed below, evidence shows that GINSTER operated the **Subject Website** and others and profited from their operation. Specifically, the evidence shows that GINSTER used his name and email address when he purchased the domain name and other services for the **Subject Website**. Further, the evidence shows that proceeds of the investment fraud from the **Subject Website** were sent to an account at Coinbase, Inc. in the name of GINSTER. Some of these funds were then converted from bitcoin to US dollars and wired to GINSTER's personal bank account.

20. The evidence in this case, including data and documents seized from GINSTER's residence pursuant to a search warrant executed on February 23, 2021, show that GINSTER maintained on his computer a bitcoin wallet that collected deposits from "investors" solicited through the **Subject Website**. An analysis of the flow of cryptocurrency into and out of the wallet shows that funds deposited to the wallet were transferred to virtual currency exchangers such as Coinbase and LocalBitcoins, as well as to gambling websites. Some of the funds were then transferred into GINSTER's personal bank account at Carrollton Bank.

21. Finally, the evidence shows that GINSTER set up and operated the **Subject Website** from his personal residence in Corona, California ("**Corona Residence**"), according to IP addresses captured by the companies he used to operate the website.

22. Records received from Charter Communications obtained pursuant to a subpoena indicated that the **Corona Residence** was assigned the IP address 76.170.245.112 beginning on April 5, 2020 and ending on October 1, 2020. As detailed below, accounts used to operate the **Subject Website** and the Coinbase account in GINSTER's name, used to convert proceeds of the fraud to US dollars, was accessed from the **Corona Residence** IP address 76.170.245.112.

II. Socialprofimatic.com

23. Individuals that wish to purchase an internet domain name are required to purchase those names through a domain name registration company. The company Namecheap provides domain name registration services. According to records received from Namecheap, GINSTER created an account with Namecheap on February 11, 2010.

24. The Namecheap records show that on February 18, 2018, the GINSTER Namecheap account purchased the domain name for the **Subject Website,** "socialprofimatic.com." The **Subject Website** is no longer available on the Internet; however, I was able to review its contents via numerous YouTube videos and from an archived version accessible on Archive.org[2].

25. From review of these YouTube videos and archived versions of the **Subject Website**, I was able to view a section of the site titled, "*How Does The Social Profimatic System Work For Me?*" The Social Profimatic website indicated that it would pay an investor 8% of

[2] *see https://web.archive.org/web/20180902054903/https://socialprofimatic.com/*

their total investment every day. This works out to a user doubling their investment in less than 13 days. According to Investopedia, the average annual return for the S&P 500 from 1957 to 2018 was approximately 8% per year.[3] Social Profimatic claimed to pay 8% per day.

26. The **Subject Website** further explained, "*After you have your deposit made, we start creating & fulfilling social media marketing orders behind the scenes day and night on your behalf!*" The website implied that this program would be long running, with statements such as, "*This will be JOB REPLACING income, the income that will pay you every hour of every day even when your [sic] sleeping or on holiday!*" (emphasis in original). And with respect to referrals, the website indicated, "*You'll get paid 10% whenever a referral directly signs up under you and makes their deposit FOR THEIR LIFETIME*" (emphasis in original).

27. The **Subject Website** indicated that withdrawals could be made at any time, "*You can request your profits any time you want and they'll be INSTANTLY paid to your Bitcoin/Litecoin wallet.*" This statement was shown to be false when, on approximately March 28, 2018, the **Subject Website** stopped fulfilling requests from users to withdraw funds with no warning or explanation. At its conclusion on March 28, 2018, the **Subject Website** had operated for approximately 38 days.

28. An IRS-CI computer investigative specialist tasked with analyzing devices seized during the search of GINSTER's residence identified an electronic data file labeled "mainwallet." I used Electrum, a popular bitcoin wallet program, to access the "mainwallet" file. The file required a password to gain access. I entered a password that consisted of the name "Ginster" with numbers and a special character, a password I saw that GINSTER used often,

[3] *see https://www.investopedia.com/ask/answers/042415/what-average-annual-return-sp-500.asp*

according to multiple files found on his computers. After accessing mainwallet, I exported the transaction history and a list of bitcoin addresses contained within the wallet. Review of this export revealed that between February 21, 2018 and May 14, 2018, during and around the time the **Subject Website** was active, the bitcoin wallet received 9,026 deposits of bitcoin, valued at the time at approximately $844,667.93. Based on the timing of the investments, and the analysis of the flow of funds into and out of the "mainwallet," and the lack of any other sources of funds for GINSTER, I believe that substantially all of the funds received were investments in the **Subject Website**. The analysis of the wallet shows that bitcoin valued at approximately $215,019.95 was transferred from the wallet to GINSTER's Coinbase account. Another $91,293.50 in bitcoin was transferred to a Finnish company called "LocalBitcoins" (Localbitcoins.com). Additional transfers of bitcoin were sent to Coinpayments.net ($59,255.46) an Estonian cryptocurrency payment processor and Freebitco.in ($22,173.72), a cryptocurrency gambling website of undisclosed ownership. None of the funds appear to have been used for "creating and fulfilling social media marketing orders" or any other uses as claimed by the **Subject Website**.

29. Review of the records provided by Coinbase indicated that GINSTER provided Coinbase with a photo of himself, an image of his driver's license, and an image of his passport. I have compared the photos GINSTER provided to Coinbase with a photo of GINSTER I received from the California Department of Motor Vehicles (DMV) and the photos appear to be the same person, and I have confirmed that the driver's license submitted to Coinbase corresponds with GINSTER's California-issued driver's license. The address listed in the California DMV records for GINSTER is the **Corona Residence**. On February 23, 2021, I was present at a search warrant on the **Corona Residence**. I observed GINSTER at the residence and

the aforementioned photos match the individual identified at the **Corona Residence** as GINSTER.

30. The Coinbase records also detail the IP addresses that were captured when the account was accessed. The records indicated that IP address 76.170.245.112 was the only non-Coinbase controlled IP address to access GINSTER's Coinbase account from April 24, 2020 to September 10, 2020. As mentioned previously, records received from Charter Communications indicated that at the time the Coinbase account was accessed, 76.170.245.112 was assigned to the **Corona Residence**.

31. I interviewed a resident of the Northern District of California (hereafter "R.K.") that invested in SocialProfimatic. Review of R.K.'s Coinbase records showed that R.K. continuously withdrew and redeposited his earnings into SocialProfimatic. Although R.K. estimated he invested less than $100 of his own money, his Coinbase records indicated larger transfers. It is unclear whether these larger transfers were due to profits he made from SocialProfimatic or if the funds he invested were larger than he estimated. Nevertheless, on March 6, 2018, R.K. used his Coinbase account to send 0.0468793 bitcoin ($502.06) to bitcoin address 1AZ6PBRgLQSj5wvRHUVK6GUs31Z3sLdMaF for the purpose of investing in SocialProfimatic. 1AZ6PBRgLQSj5wvRHUVK6GUs31Z3sLdMaF is one of the addresses contained within the "mainwallet" bitcoin wallet. R.K. stated that he saw YouTube videos encouraging people to invest in Socialprofimatic.com, claiming that if they invested and stayed with the investments, they would grow. R.K. said that at the time, he was unemployed and needed money, and believed that he could make quick cash from investing in Socialprofimatic. R.K. stated that he lost all of his funds when SocialProfimatic became unresponsive. R.K.

sought help by attempting to contact customer support at SocialProfimatic but R.K. received no response.

32. In summary, Social Profimatic began operations on approximately February 18, 2018 and represented that it would pay investors 8% of their investment amount per day. The solicitation for the investment also represented that invested funds would be used immediately for "creating & fulfilling social media marketing orders behind the scenes day and night." The Social Profimatic website indicated that investors could withdraw their profits at anytime which turned out to be false when, on March 28, 2018, Social Profimatic stopped honoring withdrawal requests from investors. During the approximate 38 days of operation, Social Profimatic received approximately $844,667.93 from investors. The evidence indicates that GINSTER was responsible for purchasing the Social Profimatic domain name and GINSTER transferred bitcoin valued at more than $215,019.95 into his Coinbase account. The Coinbase and Carrollton Bank records indicated that GINSTER converted the bitcoin he received as a result of the Social Profimatic fraud to USD and wired $78,057.91 of fraud proceeds into his personal bank account. Finally, GINSTER's Coinbase account was accessed exclusively from an IP address that was assigned to the **Corona Residence**.

III. Additional Suspected Fraudulent Websites Linked to GINSTER

a. MyMicroProfits.com

33. Namecheap records show that GINSTER used his Namecheap account to purchase the domain name MyMicroProfits.com on March 4, 2020. Review of bitcoin transfers to wallets GINSTER used to administer My Micro Profit deposits and withdrawals indicated that My Micro Profits began operation on or about June 1, 2020. The My Micro Profits website advertised, "*We will pay you INSTANT income every 60 minutes on complete autopilot!*"

(emphasis not added). The My Micro Profits website further stated that the investor would earn "*0.13% Hourly for lifelong*." Note that a return of 0.13% per hour would yield a return of 3.12% per day.

34. I have analyzed bitcoin wallets found by an IRS-CI digital forensics expert during a forensic examination of GINSTER's computers and external hard drives seized from his residence during the February 23, 2021 search. I identified a bitcoin wallet labeled "my micro profits deposits" that appears to have been used to accept deposits from "investors" in MyMicroProfits.com.

35. The "my micro profits deposits" wallet received 296.68843691 bitcoin valued at the time of transfer at $2,787,308.92. The wallet sent 193.8032297 bitcoin valued at $1,792,821.60 to bitcoin address that I have not identified. Many of these addresses likely belong to investors, who withdrew funds during the period that MyMicroProfits allowed withdrawals. GINSTER also sent 22.5 bitcoin ($210,805.65) to two wallets he controlled that appeared to be used to provide withdrawals to investors during the period that MyMicroProfits allowed withdrawals.

36. GINSTER sent the remaining funds, 78.5298083 bitcoin ($778,837.29) to bitcoin wallets that he controlled. Two of the wallets, labeled "sendingwallet" and "sending wallet original network," were used to provide a layer of transactions between MyMicroProfits and GINSTER's Coinbase account. For example, on July 1, 2020, GINSTER sent 4 bitcoin ($36,615.80) to the wallet labeled "sendingwallet." Approximately 40 minutes later, GINSTER sent 4.17635559 bitcoin ($38,230.15) from the "sendingwallet" to his Coinbase account.

b. Automaticbitcome.com

37. Namecheap records indicated that GINSTER used his Namecheap account to purchase the domain name "automaticbitcome.com" on January 10, 2017. I have reviewed archived versions of the Automatic Bitcome website, which claims that capital received from its investors would be used to loan money to businesses in need. The site stated that individuals that deposited funds to Automatic Bitcome would receive 5% of their total deposit per day for a total of 60 days.

38. I analyzed bitcoin wallets IRS-CI computer experts found during a forensic examination of GINSTER's computers and external hard drives seized from his residence during the February 23, 2021 search. I identified a bitcoin wallet labeled "automaticbitcomereceive" and a second wallet labeled "instaprofitsystembiz" that appear to have been used to accept deposits from "investors" in AutomaticBitcome.com. These wallets received 173.9679442 bitcoin valued at $668,948.14. These wallets sent 66.58666512 bitcoin ($258,652.32) to LocalBitcoins and 9.17343471 bitcoin ($$34,997.92) to GINSTER's Coinbase account. The wallets sent 91.75262177 bitcoin ($355,676.02) to unattributed bitcoin addresses many of which likely belong to investors that were able to withdraw while the platform was responsive.

39. The website BeerMoneyForum.com, a forum where users discuss online money making opportunities, detailed the Automatic Bitcome investment opportunity. The forum's users indicated that Automatic Bitcome stopped paying investors on or about March 14, 2019. Automatic Bitcome did not warn investors before ending payouts according to complaints on BeerMoneyForum.com and YouTube. Automatic Bitcome could not have fulfilled its representations that it would pay investors 5% for 60 days because it was only operational for 44

days and therefore, even the earliest investor was not able to receive 60 days of interest payments.

40. The website trustpilot.com detailed multiple negative reviews for Automatic Bitcome. For example, one individual stated, "*FAKE SITE – DOES NOT PAY – ONLY STEALS MONEY – NO ANSWERS FROM 'SUPPORT'* ." Another individual stated, "*sadly lost my investment*."

41. The Automatic Bitcome website indicated that Automatic Bitcome was registered as a United Kingdom company with registration number 11800127. UK company registration records are available through the UK government website, https://find-and-update.company-information.service.gov.uk. I searched for Automatic Bitcome on this site and found that it was registered as a United Kingdom company and had registration number 11800127. Review of the filings revealed that Automatic Bitcome was registered on January 31, 2019 and had only one Company Director, "Ryan Ginster", who was listed as a resident of the United States with a date of birth of January of 1987. GINSTER likely recognized that his name appeared on the Automatic Bitcome filings because a day later, on February 1, 2019, a document was filed that changed the Company Director name from "Ryan Ginster" to "Gabe Ginster." On Feb. 25, 2019, another form was filed to change the name from "Gabe Ginster" to "Gabe Newell."

42. Individuals who research websites often conduct a public "Whois" search to identify the person that operates a particular website. Records received from Namecheap indicated that although GINSTER used his own name when he first registered an account with Namecheap in 2010, he used the name "Ryan Oakley" as the contact person for the Automatic Bitcome website. Whois records often include an organization or a company name that owns the

website. The Namecheap records indicated that the organization associated with Automatic Bitcome was "Create My Home Business".

43. I identified a Facebook page in the name of Ryan Oakley that contained links to the websites "createmyhomebusiness.com" and "buildweeklypaychecks.com." The Namecheap records indicated that GINSTER purchased the domain names createmyhomebusiness.com and buildweeklypaychecks.com. Photos of Ryan Oakley displayed on the Ryan Oakley Facebook page appeared to be the same person as the person pictured on GINSTER's passport copy provided to Coinbase and the driver's license photo I received from the California DMV. Further, I observed GINSTER at the residence and the aforementioned photos match the individual identified at the **Corona Residence** as GINSTER.

44. Records received from Facebook indicated that the Ryan Oakley Facebook account was created on July 26, 2010. This indicates that GINSTER first used the Ryan Oakley alias in 2010. On May 2, 2020, the Ryan Oakley Facebook account was accessed from the IP address 76.170.245.112. As indicated previously, Charter Communications assigned 76.170.245.112 to the **Corona Residence** from April 2020 to October 1, 2020.

45. In summary, the evidence shows that GINSTER used the names "Gabe Ginster," "Gabe Newell," and "Ryan Oakley" as aliases. Based on my training and experience, aliases are used to hide the identity of the individual that is actually responsible for the criminal conduct.

c. eProfitHub.io

46. The Namecheap records indicated that GINSTER used his Namecheap account to purchase the domain name "eProfitHub.io." The eProfitHub website indicated that it was launched on February 4, 2020. The eProfitHub website, which I have viewed, advertised, "*Instant Crypto Income Paid to YOU Every 60 Minutes*" (emphasis not added). The eProfitHub

website further stated that investors would receive 0.25% hourly for 1,440 hours (60 days). A return of 0.25% per hour for 60 days equates to a 6% gain per day. eProfitHub stopped honoring withdrawal requests from investors on March 7, 2020 with no notice according to complaints by investors on YouTube. As indicated above, the site was operational from February 4, 2020 to March 7, 2020, approximately 32 days, therefore none of the investors could have received 60 days of payments.

47. I reviewed emails messages received pursuant to a search warrant to Google for the email account digitalsoftwearllc@gmail.com, an email account that GINSTER uses for personal matters including the creation of his personal Facebook account and his Coinbase account. On January 26, 2020, GINSTER received an email from admin@hyips4u.com that confirmed his purchase of UK Incorporation documents for eProfitHub.io LTD. The service was priced at $309.00 and included passport and utility documents. On February 5, 2020, GINSTER received an email from gs2581368@gmail.com with the name Hyips4u Admin that had attached a UK passport in the name of Hayden Hudson and a water bill in the same name. A search of EPROFITHUB.IO LTD on the Companies House website shows that Hayden Hudson is listed as the eProfitHub.io LTD Director. Review of an archived version of eProfitHub.io as it appeared on March 2, 2020, showed GINSTER listed that eProfitHub.io LTD was registered in the U.K.

48. I analyzed bitcoin wallets IRS-CI computer experts found during a forensic examination of GINSTER's computers and external hard drives seized from his residence during the February 23, 2021 search. I identified a bitcoin wallet labeled "eprofithub withdrawals" and a second wallet labeled "eprofithub deposits" that appear to have been used to accept deposits from "investors" in eProfitHub.io. These wallets received 80.33639214 ($738,880.89). The two wallets sent 55.00608638 bitcoin ($503,705.17) to unattributed wallets, many of which likely

belong to investors who were able to withdraw while eProfitHub.io was operational. The remaining bitcoin was sent to wallets controlled by GINSTER including 12.96381999 bitcoin ($118,543.88) GINSTER sent to a wallet found on GINSTER's devices labeled "trezorreceiveonly." From my training and experience as well as from the website trezor.io, I know that a Trezor is a device commonly used to store bitcoin and other cryptocurrencies.

49. During the search of GINSTER's residence, agents found a document with 24 words written on it in a suitcase located in a closet in GINSTER's master bedroom. The face of the document read "Welcome Ledger Nano S." From my training and experience and the website ledger.com, I know that, similar to the Trezor, the Ledger Nano S is a hardware wallet for storing bitcoin and other cryptocurrencies. I also discovered that the 24 seed words written on the document and the seed words for the "trezorreceiveonly" wallet are the same.

50. Pursuant to the search warrant, agents used Electrum software and the 24 word recovery phrase to recover access to the wallet. Agents discovered that the wallet contained 59.65744106 bitcoin. Agents seized this bitcoin by transferring it to an IRS-CI controlled bitcoin wallet pursuant to the search warrant.

51. On or about June 13, 2020, a victim filed a complaint with the Internet Crime Complaint Center that detailed a loss of $5,432.40. The victim sent bitcoin as instructed on eProfitHub and expected to make a return of $19,556.64 in 60 days. The victim stated that he was subsequently unable to access the site and has hired an attorney.

d. YourNetProfits.com

52. The Namecheap records indicated that GINSTER used his Namecheap account to purchase the domain name "yournetprofits.com." According to an individual who posted a review of Your Net Profits on July 24, 2020, the Your Net Profits website was first launched on

or about July 19, 2020. The Your Net Profits website advertised, "*Get Paid Instant Crypto Every 60 Minutes From a Real Website Network*." The Your Net Profits website further indicated that the investor would receive 0.15% hourly for a lifetime. A return of 0.15% per hour would yield a return of 3.6% per day. On September 9, 2020, I reviewed the "Latest Payouts" page of Your Net Profits and saw that the last withdraw occurred on or about August 3, 2020. From review of YouTube comments, it appears Your Net Profits ceased honoring investor withdraw requests with no notice to investors, thus unfulfilling the representation that payments would be 0.15% per hour for a lifetime.

53. I analyzed bitcoin wallets IRS-CI computer experts found during a forensic examination of GINSTER's computers and external hard drives seized from his residence during the February 23, 2021 search. I identified a bitcoin wallet labeled "your net profit deposits" and a second "your net profits withdrawals" that appear to have been used to accept deposits from "investors" and make payments to "investors" in YourNetProfits.com. The "your net profit deposits" wallet received 68.69282443 ($657,398.73). The two wallets sent 38.37690945 bitcoin ($408,989.66) to unattributed wallets, many of which likely belong to investors who were able to withdraw while YourNetProfits.com was operational. Most of the remaining bitcoin, 29.74020874 ($328,792.88) was sent to "sendingwallet", the previously mentioned wallet that was used to add a layer between MyMicroProfits.com deposits and GINSTER's Coinbase wallet.

54. Review of GINSTER's Coinbase account showed that he converted the bitcoin he received from his operation of the fraudulent HYIP websites into USD and wired those funds to his personal bank account at Carrollton Bank. I used the "Last Out" rule to identify wire

transfers that contained fraud proceeds.[4] Based on this analysis, I identified 25 wire transfers, totaling $697,672.47. Of that total, I identified $641,260.81, or 92% of the total, that originated from the five HYIP websites.

CONCLUSION

55. In summary, the evidence shows that GINSTER used the **Subject Website** and other websites to direct investors to send funds to bitcoin addresses controlled by him. GINSTER then transferred bitcoin from those addresses to an account he held at Coinbase as well as to other currency exchangers, gambling websites, and elsewhere. GINSTER used Coinbase to convert bitcoin to US Dollars and then transferred those monies to a bank account held personally by GINSTER.

56. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that the defendant GINSTER has committed violations of law to include Title 18, United States Code, Section 1343 (Wire Fraud), and Title 18 United States Code, Section 1956 (Engaging in Monetary Transactions to Disguise or Conceal). I therefore request that you issue the criminal complaint and arrest warrant.

REQUEST FOR SEALING

57. I further request the Court order all papers in support of this application, including the affidavit and arrest warrant, be sealed until further order of the Court. There is good cause to seal these documents because their premature disclosure may give target(s) an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

[4] The Last Out rule presumes that funds not identified as criminal proceeds are expended first.

Dated:

/s/
JEREMIAH HAYNIE, SPECIAL AGENT
Internal Revenue Service - Criminal Investigation

Dated:

HON. JACQUELINE SCOTT CORLEY
United States Magistrate Judge